FREE GUIDE · MIKE STRASSBURG IT SERVICES & SUPPORT

How to Spot a Scam Email

Scam emails try to trick you into clicking, paying or giving away a password. Here's how to catch them.

GOLDEN RULE **Stop. Check. Then act.** If an email makes you rush, panic or pay, slow down. A real company will still be there in 10 minutes.

SPOT THE FAKE

From: Parcel Delivery (1) notice@parcel-track-alerts.top
Subject: FINAL NOTICE: Package on hold (2)

Dear Customer, (3)
We were unable to deliver your package. A $1.99 redelivery fee is required within 24 hours or it will be returned. (4)

Pay & Reschedule (5)

1. Strange sender address
2. Scary, all-caps subject
3. Doesn't use your name
4. Small fee + a deadline
5. Button leads to a fake site

NOT SURE? DO THIS

1. **Don't click, reply or call**
   Leave the email alone until you've checked it.
2. **Go there yourself**
   Type the company's web address or open their app instead of using the link.
3. **Call a number you trust**
   Use the number on your card, bill or their real website, not the one in the email.
4. **Report it and delete it**
   Use "Report phishing" or "Junk" in Outlook or Gmail.

10 RED FLAGS

Check who it's really from
Look past the name to the actual address. "Your Bank" ‹alerts@yourbank-secure.info› is not your bank.

Read the web address carefully
The real site is just before the first "/". yourbank.com/login is real. yourbank.com.verify-login.net is fake.

Gift cards, wire transfers or crypto
No real business or bank asks to be paid this way. If an email mentions gift cards, it's a scam.

Asks for passwords or codes
Real companies never ask you to email a password or read back a code they texted you.

A "quick favor" from your boss or pastor
"Are you free? I need you to grab some gift cards." Call them on a number you know before doing anything.

Hover before you click
On a computer, rest your mouse on a link to see where it really goes. On a phone, press and hold.

Rush, fear or threats
"Your account will be closed in 24 hours." "Unusual sign-in." "Final notice." Pressure is the #1 warning sign.

A bill for something you didn't buy
Fake "renewal" or "order" emails with a phone number to call and cancel. Calling it connects you to the scammer.

Unexpected attachments or QR codes
Don't open surprise files (.zip, .html, "enable editing") or scan QR codes in emails.

Generic greeting, odd details
"Dear Customer," a slightly-off logo or strange wording. Scams are well written now, so don't rely on typos alone.

Already clicked? Don't panic.

- → Change that password, starting with your email
- → Call your bank if you shared card info
- → Turn on 2-step verification
- → Run a virus scan, then call me

Need help?

Got a suspicious email? Forward it to me or call and I'll take a look.

CALL 218-431-1739
EMAIL mike@strassburgit.com